Guidance for Federal Employees and Retirees:

The following guidance is provided by OPM:

• Don't answer unsolicited phone calls, in-person visits or e-mails from anyone asking about federal employees or other internal information in your agency.

• Don't provide personal information or any information about your agency or how it's organized to anyone unless you know them or have verified that they're legitimate.

• Don't reveal your personal or financial information in e-mail — and don't follow links sent through e-mail.

• Do not send sensitive information over the Internet before checking a Web site's security.

• Pay attention to the URL of a Web site. Malicious Web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

• If you're unsure whether an e-mail request is legitimate, try to verify it by contacting the sender directly. Don't use contact information provided on a Web site connected to the request — instead check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group.

• Install and maintain anti-virus software, firewalls and e-mail filters to reduce some of this traffic (for more information, see:

Understanding Firewalls https://www.us-cert.gov/ncas/tips/ST04-004
Understanding Anti-Virus Software, https://www.us-cert.gov/ncas/tips/ST04-005
Reducing Spam, https://www.us-cert.gov/ncas/tips/ST04-007

• Take advantage of any anti-phishing features offered by your agency.

• Monitor your checking and other financial accounts, and immediately report any suspicious or unusual activity to your bank.

• Request a free credit report at https://www.AnnualCreditReport.com or by calling 1-877-322-8228. You're entitled by law to one free credit report per year from each of the three major credit bureaus. Contact information for the credit bureaus can be found on the Federal Trade Commission (FTC) Web site, https://www.ftc.gov/.

• Review the FTC identity theft Web site, https://www.identitytheft.gov/ . The agency lists a variety of consumer publications that have a lot of information on computer intrusions and identity theft.

• Consider placing a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call TransUnion® at 1-800-680-7289 to place this alert. TransUnion® will then notify the other two credit bureaus on your behalf.